(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号

特開平9－114946

(43)公開日　平成９年(1997)５月２日

(51)Int.Cl.[6]		識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｇ０６Ｋ	17/00			Ｇ０６Ｋ	17/00	Ｔ
Ｇ０６Ｆ	12/14	３２０		Ｇ０６Ｆ	12/14	３２０Ｃ
	15/00	３３０			15/00	３３０Ｇ
Ｇ０６Ｋ	19/07		7259－5Ｊ	Ｇ０９Ｃ	1/00	６６０Ａ
Ｇ０９Ｃ	1/00	６６０		Ｇ０６Ｋ	19/00	Ｎ

審査請求　未請求　請求項の数３　ＯＬ　（全 10 頁）　最終頁に続く

(21)出願番号　特願平7－255262

(22)出願日　平成７年(1995)10月２日

(71)出願人　390009531
インターナショナル・ビジネス・マシーンズ・コーポレイション
ＩＮＴＥＲＮＡＴＩＯＮＡＬ　ＢＵＳＩＮＥＳＳ　ＭＡＳＣＨＩＮＥＳ　ＣＯＲＰＯＲＡＴＩＯＮ
アメリカ合衆国10504、ニューヨーク州　アーモンク　（番地なし）

(72)発明者　西野　清志
神奈川県大和市下鶴間1623番地14　日本アイ・ビー・エム株式会社　大和事業所内

(74)代理人　弁理士　合田　潔　（外２名）

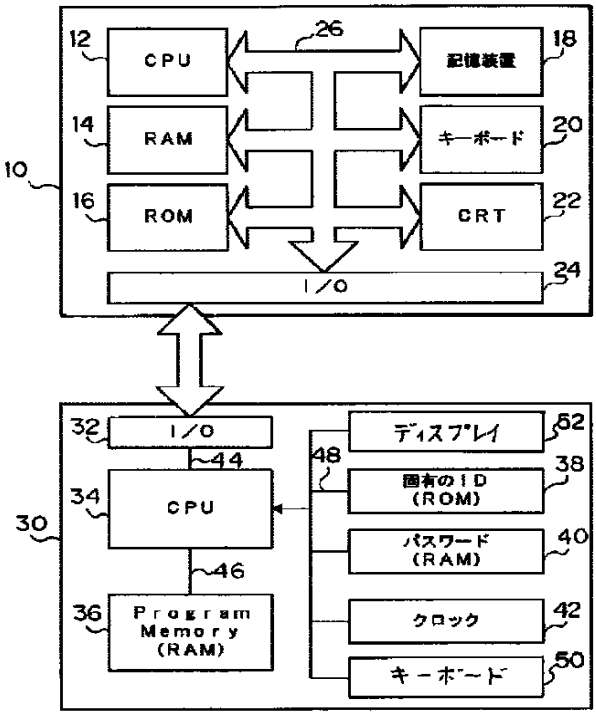
最終頁に続く

(54)【発明の名称】　ＩＣカード及び情報処理装置の認証方法

(57)【要約】

【課題】　ＩＣカードを用いて秘密性が高い情報を安全性を確保しつつ授受することを可能とする。

【解決手段】　ＩＣカード３０は、ＩＤを保持したＲＯＭ３８、クロック４２、パスワードを記憶したＲＡＭ４０、暗号化プログラム記憶したＲＡＭ３６、処理実行をするＣＰＵ３４を備え、暗号化プログラムをロードし、記憶されたＩＤ、パスワード、及びクロック４２で計数された時間ｔを読み取り、これらのＩＤ、パスワード、及び時間ｔを暗号化プログラムに従って符号化し、コンピュータシステム１０へ出力する。コンピュータシステム１０では、ＩＣカード３０からの出力を復号化してパスワードを抽出し、復号化されたパスワードと登録されたパスワードとの一致を判断し、一致のときアクセスを許可し、不一致のときアクセスを不許可とする。



【特許請求の範囲】
【請求項１】　情報処理装置に接続可能なＩＣカードにおいて、
時間を計数するクロックと、
予め定められた固有情報を表すＩＤを記憶したＩＤ記憶手段と、
前記情報処理装置への接続時に前記ＩＣカードを識別するための秘密情報を記憶するための秘密情報記憶手段と、
少なくとも前記秘密情報を符号化するための符号化処理手順を記憶するための手順記憶手段と、
前記手順記憶手段に記憶された符号化処理手順に従って少なくとも前記秘密情報を符号化する制御手段と、
を備えたＩＣカード。
【請求項２】　請求項１に記載のＩＣカードを用いて、前記ＩＣカードと情報処理装置とを接続したときに、当該ＩＣカードと前記秘密情報が予め登録された情報処理装置との間の相互の接続を認証する情報処理装置の認証方法であって、
前記情報処理装置から前記ＩＣカードへ前記秘密情報及び前記符号化処理手順を出力し、
ＩＣカードにおいて、読み取った前記秘密情報及び前記符号化処理手順を記憶し、記憶された前記秘密情報及びＩＤ情報並びにクロックにより計数した時間を読み取り、読み取った時間、秘密情報及びＩＤ情報を、記憶された符号化処理手順に従って符号化し、符号化した出力情報を前記情報処理装置へ出力し、
情報処理装置において、入力された前記ＩＣカードからの出力情報を、前記符号化処理手順に対応する復号化処理手順に従って復号し、復号された秘密情報と予め登録された秘密情報とが一致するとき、相互の接続を認める、
情報処理装置の認証方法。
【請求項３】　前記秘密情報及び符号化処理手順は、前記クロックにより計数した時間に基づく定期的な時期に前記ＩＣカード側からの指示によって変更可能であることを特徴とする請求項２に記載の情報処理装置の認証方法。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、ＩＣカード及び情報処理装置の認証方法にかかわり、特に、コンピュータや端末等の情報処理装置に接続可能なＩＣカード及びそのＩＣカードを用いてＩＣカードと情報処理装置との間の相互の接続を認証する情報処理装置の認証方法に関する。
【０００２】
【従来の技術】ユーザによって作成されたデータ等の情報を処理する装置として、ネットワークに接続された端末装置、独立して処理実行が可能なスタンドアロン型のマイクロコンピュータ、及び携帯型のマイクロコンピュータ等の装置（以下、情報処理装置という。）が知られている。この各情報処理装置は、複数のユーザが使用することができる。このような各情報処理装置上で特定の処理を実行できるが、各情報処理装置上には、個人的な電話番号や暗証番号等に挙げられるような、他に知られたくない秘密性が高い情報（以下、秘密情報という。）が保持記憶されていることがあり、登録者以外の使用者がこのような秘密情報を授受できないように安全対策（セキュリティー）が必要である。
【０００３】従来の安全対策の一例では、図６（１）に示すように、情報処理装置において処理を実行するときに、入力されたパスワードと予め登録されたパスワードとが一致するときにのみ処理実行を許可するものがある。例えば、ネットワークの端末装置からそのネットワーク自体にアクセスを求めたとき、ネットワーク側からパスワードの入力を求め、パスワードが予め登録したパスワードと一致するときに、ネットワーク側がアクセスを許可する。また、情報処理装置の他例としてはキャッシュディスペンサ（現金自動支払機）が知られており、このキャッシュディスペンサはキャッシュカードを挿入し、パスワードに相当する予め登録された暗証番号を入力することで、現金を授受することができる。
【０００４】しかしながら、パスワードが他人に知られてしまうと、誰であっても情報処理装置の処理実行が可能となる。このため、パスワードを定期的に更新することが考えられるが、安全性を考慮して短期間で更新するようにすると使用者側の負担が増大し、負担軽減のため更新期間を長くするとリスクが増大する。
【０００５】この問題を解消するため、図６（２）に示すように、情報処理装置において処理を実行するときに、情報処理装置に物理的な装置（ハードワイヤーキー：Ｈ／Ｗキー）を付加するようにすれば、この物理的な装置を有するときにのみ情報処理装置で処理実行が可能となる。
【０００６】しかしながら、物理的な装置は、リバースエンジニアリングとして知られているように、同一装置を作成することが比較的容易である。例えば、ＲＯＭを備えることでこのＲＯＭの内容に従って認証するような物理的な装置はＲＯＭを複写することで同一装置を作成することが可能であり、論理回路等で物理的な装置を構成するときはその出力信号を検出することで同一の装置を作成できる。このように、同一の物理的な装置が作成できれば誰であっても情報処理装置の処理実行が可能となる。
【０００７】ところで、近年の情報産業の進展によって、別個の装置をケーブル等で接続した外部装置として機能した処理装置そのものをＩＣカード内に凝縮させて、端末に接続することによって外部接続機器として機能する、一定の情報を記憶保持可能なメモリカードやＬ

ＳＩカード等のＩＣカードが知られている。

【０００８】このＩＣカードを用いた、通信の安全保護確保を目的とした通信システムのハードウェア又は構成要素を確認するためのものとして、端末確認方式がある（特公平４－５１８６４号公報参照）。この技術では、メモリカードに記憶されたパスワード等の秘密番号をキーとして用い、第１の端末のキーに基づいて暗号化された乱数が第２の端末に出力される。次に、第２の端末は、暗号化された番号（乱数）を予め記憶されたそのキーを使って解読し、キーが同一の場合には乱数を生成し、その乱数の誘導形を使ってそのキーを暗号化し、第１の端末への応答を生成し出力する。次に、第１の端末は、その乱数をキーとして使って、その応答がそのキーを暗号化したものであるかどうかを決定する。その応答がキーの暗号である場合、第２の端末は確認されたことになり、キーの暗号でない場合、その端末は未確認となり、通信が停止される。

【０００９】

【発明が解決しようとする課題】しかしながら、従来の端末確認方式では、カード側と端末側との各々のキーは固定的であり、パスワードに相当するキー自体が知られた場合には、誰であっても情報処理装置の処理実行が可能となる。このため、上述のようにキーを、安全性を考慮して短期間で更新する必要があり、使用者側の負担が増大する。

【００１０】本発明は、上記事実を考慮して、秘密性が高い情報を安全性を確保しつつ授受することが可能なＩＣカード及び情報処理装置の認証方法を得ることが目的である。

【００１１】

【課題を解決するための手段】上記目的を達成するために本発明のＩＣカードは、情報処理装置に接続可能であり、時間を計数するクロックと、予め定められた固有情報を表すＩＤを記憶したＩＤ記憶手段と、前記情報処理装置への接続時に前記ＩＣカードを識別するための秘密情報を記憶するための秘密情報記憶手段と、少なくとも前記秘密情報を符号化するための符号化処理手順を記憶するための手順記憶手段と、前記手順記憶手段に記憶された符号化処理手順に従って少なくとも前記秘密情報を符号化する制御手段と、を備えている。このＩＣカードを識別するための秘密情報としては暗証番号やパスワードがある。また、符号化処理手順には、暗号化プログラムや符号化プログラムがある。

【００１２】なお、少なくとも前記秘密情報を符号化するための符号化処理手順を複数記憶した複数の手順記憶手段、をさらに備えてもよい。この場合、制御手段は、前記複数の手順記憶手段に記憶された複数の符号化処理手順から１つの符号化処理手順を選択し選択した符号化処理手順に従って少なくとも前記秘密情報を符号化する。

【００１３】また、本発明の情報処理装置の認証方法は、前記ＩＣカードを用いて、ＩＣカードと情報処理装置とを接続したときに、当該ＩＣカードと秘密情報が予め登録された情報処理装置との間の相互の接続を認証するためのものである。

【００１４】情報処理装置からは、ＩＣカードへ予め登録された秘密情報及び符号化処理手順が出力される。ＩＣカードでは、情報処理装置から出力された秘密情報及び符号化処理手順を読み取った後に記憶する。この時点でＩＣカードは情報処理装置に対して接続認証のためのキーとして機能する。このＩＣカードでは記憶された秘密情報及びＩＤ情報並びにクロックにより計数した時間を読み取る。この読み取った時間、秘密情報及びＩＤ情報は、その時間におけるＩＣカード固有の情報になる。この読み取った時間、秘密情報及びＩＤ情報を、記憶された符号化処理手順に従って符号化し、符号化した出力情報を情報処理装置へ出力する。従って、情報処理装置に入力される出力情報は、その時間におけるＩＣカード固有の情報が符号化された特有の情報になる。

【００１５】情報処理装置では、入力されたＩＣカードからの出力情報を、符号化処理手順に対応する復号化処理手順に従って復号する。この復号された秘密情報が、情報処理装置側からの出力の返信であるときにＩＣカードは認証すべきものであるので、復号された秘密情報と予め登録された秘密情報とが一致するとき、相互の接続を認める。

【００１６】なお、前記秘密情報及び符号化処理手順は、前記クロックにより計数した時間に基づく定期的な時期に前記ＩＣカード側からの指示によって変更可能である。ＩＣカードはクロックを有しており、自らが秘密情報及び符号化処理手順の変更時期を計数できる。従って、安全性を確保するための定期的な時期における秘密情報及び符号化処理手順の変更に際して、長期間を経過することなく予め定めた定期的な変更が可能である。

【００１７】

【発明の実施の形態】以下、図面を参照して本発明の実施の形態の一例を詳細に説明する。本実施の形態は、情報処理装置としてのコンピュータシステムとＩＣカードとの間において、情報の授受を行って、コンピュータシステムへのアクセス（実行処理）を許可する場合に本発明を適用したものである。

【００１８】図１に示すように、本実施の形態にかかる、情報処理装置の認証方法を処理するための装置構成は、コンピュータシステム１０、及びＩＣカード３０からなる。コンピュータシステム１０は、ＣＰＵ１２、ＲＡＭ１４、ＲＯＭ１６、記憶装置１８、キーボード２０、ＣＲＴ２２、入出力装置（Ｉ／Ｏ）２４及びこれらをコマンドやデータを授受可能なように接続したバス２６から構成されている。この記憶装置１８には、予め定めた符号化処理を行うための暗号化プログラムが記憶さ

れている（詳細後述）。また、記憶装置１８には登録されたパスワードが記憶される。

【００１９】ＩＣカード３０は、入出力部（Ｉ／Ｏ）３２を備えており、この入出力部３２とコンピュータシステム１０の入出力装置２４に接続される。ＩＣカード３０の入出力部３２には、バス４４を介して演算ユニットであるＣＰＵ３４が接続されており、このＣＰＵ３４にはバス４６を介して符号化プログラムを一時的に記憶するためのプログラムメモリである書換可能なＲＡＭ（詳細後述）３６が接続されている。また、ＣＰＵ３４には、ＩＣカード３０の製造時に記録された固有の情報が格納されたＲＯＭ３８、パスワードを格納するための書換可能なＲＡＭ４０及び内蔵時計として機能するクロック４２が、バス４８を介して接続されている。なお、ＲＯＭ３８には、ＩＣカード３０の固有の情報、例えば製造番号やＩＣカードの種類を表すラベル等のＩＤが製造時に予め書き込まれている。

【００２０】また、本実施の形態のＩＣカード３０は、上記の入出力部（Ｉ／Ｏ）３２、ＣＰＵ３４、ＲＡＭ３６、ＲＯＭ３８、ＲＡＭ４０及びクロック４２を基本主要素とし、さらなる構成として、パスワードを入力するために用いられる入力手段としてのキーボード５０及びデータやコマンドを表示する表示手段としてのディスプレイ５２を有している。これらキーボード５０及びディスプレイ５２は、バス４８に接続されている。ＩＣカード３０がキーボード５０を有することによってパスワード、コマンド及びデータのＩＣカードによる入力が可能となり、ディスプレイ５２を有することによってパスワード、コマンド及びデータのＩＣカード上における確認が可能となる。なお、キーボード５０及びディスプレイ５２は、ＩＣカード３０の必須構成とするものではなく、キーボードのみまたはディスプレイのみであってもよい。また、パスワード等を入力するためにコンピュータシステム１０側のキーボード２０及び表示確認のためにＣＲＴ２２を用いてもよいことは勿論である。

【００２１】図７には、上記ＩＣカード３０の一例として、ＩＣカード３０の外観斜視図を示した。図７のＩＣカードは、クレジットカードサイズの大きさの着脱式装置（所謂、ＰＣＭＣＩＡカード：ＰＣＭＣＩＡ規格に準拠した拡張用のカード）であり、ケーシング３０Ａ内に上記入出力部３２、ＣＰＵ３４、ＲＡＭ３６、ＲＯＭ３８、ＲＡＭ４０及びクロック４２が内蔵されている。また、ケーシング３０Ａの上面に英数字が対応された複数のボタン型スイッチからなるキーボード５０及びＬＣＤユニットで形成されたディスプレイ５２が設けられている。また、ケーシング３０Ａの側面部分には端子３２Ａが設けられており、端子３２Ａは入出力部３２の外部への接続端子として機能する。すなわち、このＩＣカード３０はコンピュータシステム１０側に設けられているカードスロット（図示省略）に装填され、端子３２Ａがカードスロット内の端子（図示省略）に接続される。

【００２２】次に、コンピュータシステムとＩＣカードとの間の認証の手順を図２及び図３を参照して説明する。

【００２３】コンピュータシステム１０では、図２に示すように、ステップ１０２において入出力装置２４にＩＣカード３０の入出力部３２が接続されたか否かを判断することによって、コンピュータシステム１０にＩＣカード３０が装着されたか否かを判断する。このステップ１０２において肯定判断されると、ＩＣカード３０が装着されているので、次のステップ１０４へ進み、既に登録され、記憶装置１８に記憶されているパスワード、及び暗号化プログラムを読み取って、ＩＣカード３０へ出力する。

【００２４】ＩＣカード３０では、コンピュータシステム１０からの入力が有るまで、ステップ２０２を繰り返し実行する。コンピュータシステム１０から信号が入力されると（図２のステップ１０４による）、ステップ２０２で肯定判断され、次のステップ２０４へ進む。ステップ２０４では、コンピュータシステム１０から出力されたパスワード、及び暗号化プログラムを受け取って、パスワードはＲＡＭ４０へ、暗号化プログラムはＲＡＭ３６へ格納する。次に、格納された暗号化プログラムを実行可能な状態に読み取る（所謂、ロードする）。

【００２５】以上の処理が終了した段階で、ＩＣカード３０はセキュリティキーとしての機能を有することになる。すなわち、ＩＣカード３０はパスワード及び後述する暗号化プログラムに従ってパスワードを出力可能な状態になっており、ハードワイヤー装置を装備したコンピュータシステムと同等のシステムとして機能する。

【００２６】なお、本実施の形態のＩＣカード３０はキーボード５０を有しているので、キーボード５０によってパスワードを入力することも可能である。この場合、図２のステップ１０４では暗号化プログラムのみを出力する。また、図３のステップ２０４ではコンピュータシステム１０から出力された暗号化プログラムを受け取って、ＲＡＭ３６へ格納する。また、図示は省略したが、図３のステップ２０４の前または後にパスワードの入力処理を追加する。ＩＣカード３０のキーボード５０によって入力されたパスワードはＲＡＭ４０へ格納する。また、この場合のパスワードはディスプレイ５２に表示させるようにしてもよく、秘密性を高めるため入力されたことのみを記号で表示させる等のようにマスクしてもよい。

【００２７】次のステップ２０６では、ＲＯＭ３８に記憶されたＩＤ、ＲＡＭ４０に記憶されたパスワード、及びクロック４２で計数されている時間ｔを読み取る。次のステップ２０８では、以下に説明するように、これらのＩＤ、パスワード、及び時間ｔを暗号化プログラムに従って符号化した出力情報を生成し、次のステップ２１

０においてコンピュータシステムへ出力する。なお、生成された出力情報のコンピュータシステム１０への出力は、コンピュータシステム側から要求された場合に行うようにしてもよい。

【００２８】ここで、ステップ２０８において実行される符号化処理の一例を説明する。本実施の形態では、パスワードを符号化するために、コンピュータシステム１０からのパスワードＰ、ＩＣカード３０の固有の情報であるＩＤ及びクロックによる時間ｔを用いている。これらのパスワードＰ、ＩＤ及び時間ｔを次の（１）式に従って符号化することによって出力情報Ｇを得る。

【００２９】

$$G = RND\{F(P, ID, t)\} \quad \cdots (1)$$

但し、Ｆ　　：加減乗除の組み合わせからなる関数

ＲＮＤ：ランダム関数（一般的なプログラム言語で用いられるもの）

【００３０】このようにしてＩＣカード３０はパスワードが符号化された乱数を出力情報としてコンピュータシステム１０へ出力する。

【００３１】なお、コンピュータシステムにおける時間とクロックによる計数時間とは同一性を高めるため、略一致させることが好ましい。

【００３２】次に、コンピュータシステム１０では、ＩＣカード３０から信号（出力情報）が入力されるまで、図２のステップ１０６を繰り返し実行する。ＩＣカード３０から出力情報が出力されると、コンピュータシステム１０は、図２のステップ１０６において肯定判断され、ステップ１０８へ進む。ステップ１０８では、ＩＣカード３０からの出力情報を読み取ると共に、復号化処理をする。この復号化処理の実行によって出力情報に含まれているパスワードを抽出できる。すなわち、ＩＣカード３０から入力された出力情報は前記ステップ１０４においてＩＣカード３０へ出力した暗号化プログラム（本実施の形態では上記の式（１）による処理）に従った情報（乱数）であるので、復号化処理は容易である。例えば、前記式（１）の逆関数によって復号することができる。なお、コンピュータシステム１０は暗号化プログラムによって生成される情報を復号化する復号プログラムを予め記憶してもよい。

【００３３】次のステップ１１０では、復号化処理によって得られたパスワードと登録されたパスワードとが一致するか否かを判断する。パスワードが一致し、ステップ１１０で肯定判断の場合には、ステップ１１２においてコンピュータシステム１０へのアクセスを許可する。すなわち、このコンピュータシステム１０を用いての処理を可能な状態にする。例えば、コンピュータシステム１０がネットワークに接続されているときに、このＩＣカード３０をもってネットワークへアクセスしようとする場合にはログオン時のアクセス権を得ることに対応する。

【００３４】一方、パスワードが不一致となりステップ１１０で否定判断の場合には、ステップ１１４においてコンピュータシステム１０へのアクセスを不許可とし、これよりの処理を強制的に終了する。例えば、電源オフ状態にすることや、警告表示を行う。

【００３５】なお、上記のパスワード及び暗号化プログラムは定期的に新規なものに更新されることが好ましい。

【００３６】次に、以上の処理が終了した段階で、コンピュータシステム１０からＩＣカード３０を取り外し、再度ＩＣカード３０を装着した場合を説明する。この場合、コンピュータシステム側では、既にＩＣカード３０へパスワード及び暗号化プログラムの出力は終了しているので、コンピュータシステム側の図２のステップ１０４の処理、及びＩＣカード側の図３のステップ２０４の処理は不要となる。コンピュータシステム側では、ステップ１０４の処理に代えて、パスワード参照処理が実行される。すなわち、ＩＣカード３０に対して保持しているＩＤ、パスワード及び時間ｔにとって生成される出力情報の出力要求を指示する。ＩＣカード側では、ステップ２０４の処理をスキップする。これによって、コンピュータシステム１０にＩＣカード３０が装着されると、コンピュータシステム側からＩＣカードに対して出力情報の要求がなされ、ＩＣカードは生成した出力情報をコンピュータシステムへ出力する。このＩＣカードから出力された出力情報に含まれるパスワードと登録されているパスワードとを上述のように比較し一致したときにシステムへのアクセスを許可する。

【００３７】なお、本実施の形態のＩＣカード３０はキーボード５０を有しているので、キーボード５０によりパスワードを逐次入力させることも可能である。この場合には、図３のステップ２０４に代えてパスワードの入力処理を実行する。ＩＣカード３０のキーボード５０によって入力されたパスワードはＲＡＭ４０へ格納する。これによって、コンピュータシステム１０にＩＣカード３０が装着されると、コンピュータシステム側からＩＣカードに対して出力情報の要求がなされ、ＩＣカードではこれを受けてパスワードの入力処理が成され、生成した出力情報をコンピュータシステムへ出力する。このＩＣカードから出力された出力情報に含まれるパスワードと登録されているパスワードとを上述のように比較し一致したときにシステムへのアクセスを許可する。

【００３８】このように、本実施の形態では、ＩＣカード３０にＣＰＵを備え、暗号化プログラムを格納するためのＲＡＭを有することによって、ＩＣカード自体で符号化処理をすることができる。従って、秘密情報としてのパスワードは符号化されて出力することができ、ＩＣカードからの出力信号を検出することのみでは、秘密情報を検知することが不可能となり、安全性を向上させる

ことができる。また、暗号化プログラムを記憶するものとして、一時的に保持する書換え可能なＲＡＭを用いているため、暗号化プログラムそのものを変更することができ、リバースエンジニアリングを用いて物理的に複写しても、一時的な保持に留まり継続的な使用は不可能となり、安全性を向上させることができる。

【００３９】ここで、上記実施の形態では、ＩＣカード３０はクロック４２を備えているので、ＩＣカード単体で時間計測が可能である。従って、ＩＣカード３０に記憶しているパスワードについて有効期限を設定することが可能となる。この有効期限設定処理について説明する。なお、ここでは、パスワードが登録または更新されたときの時間をパスワードと共に記憶するものとする。また、有効期限は予めコンピュータシステム側で設定される、または登録時に所定の時間が設定されているものとする。

【００４０】図４には、ＩＣカードにおいて所定時間毎に実行される割り込みルーチンを示した。図４のステップ２２２では、クロック４２を読み取る。これによって、現在時間を検知できる。次のステップ２２４では、前回の更新時間または登録時間を読み取る。この登録時間はパスワードを保持記憶するＲＡＭ４０に共に記憶されている。次のステップ２２６では、上記読み取った現在時間と更新時間または登録時間を比較し、予め設定された設定時間を経過したか否かを判断する。否定判断され、設定時間以内のときはそのまま本ルーチンを終了する。一方、肯定判断の場合には、ステップ２２８において期限切れ処理が実行される。この期限切れ処理には、ＩＣカードの使用を禁止する禁止処理やコンピュータシステムへの装着時にシステム側へ期限が切れたことを報知する処理がある。なお、ＩＣカード３０に表示装置を追加して備えることによってパスワードを登録または更新してから設定時間を経過したことを警告するように表示させることが可能となる。また、コンピュータシステム１０への接続時にコンピュータシステム側から警告表示することも可能である。

【００４１】次に、上記ＩＣカード３０はクロック４２及びプログラムを記憶するための書換え可能なＲＡＭ３６を備えているので、ＩＣカード単体で時間計測が可能であると共に、パスワード更新処理実行が可能である。すなわち、ＩＣカード３０に記憶しているパスワードが所定の期間を経過すると自動的にパスワード更新処理することが可能となる。このパスワード更新処理について説明する。なお、ここでは、パスワードが登録または更新されたときの時間をパスワードと共に記憶するものとする。また、有効期限は予めコンピュータシステム側で設定される、または登録時に所定の時間が設定されているものとする。

【００４２】図５には、ＩＣカードにおいて所定時間毎に実行される割り込みルーチンを示した。図５のステップ２２２では、上記の図４の処理と同様にクロック４２を読み取り現在時間を検知する。次のステップ２２４では、前回の更新時間または登録時間を読み取る。次のステップ２２６では、上記読み取った現在時間と更新時間または登録時間を比較し、予め設定された設定時間を経過したか否かを判断する。否定判断され、設定時間以内のときはそのまま本ルーチンを終了する。一方、肯定判断の場合には、ステップ２３０においてパスワード更新処理が実行される。このパスワード更新処理は、ＩＣカード自体に更新処理実行プログラムを予め記憶しておき、自動的に更新するようにしてもよい。また、コンピュータシステムへの装着時にパスワード更新を促す処理へコンピュータシステムが移行するように指示信号を出力するようにしてもよい。

【００４３】なお、本実施の形態では、ＩＣカードの使用者が単一の場合について説明したが、複数の使用者がＩＣカードを共用することが可能である。この場合、ＩＣカードは上述のように書換え可能なＲＡＭを備えているので、パスワードを記憶するＲＡＭをテーブル化して複数のパスワードを記憶するようにすれば、各々のパスワードの安全性は確保され、複数の使用者が共同でＩＣカードを使用することができる。

【００４４】また、本実施の形態のＩＣカードは、書換え可能なＲＡＭを備えているので、パスワードの更新履歴やアクセス不許可の履歴を記憶することが可能である。このように、パスワードの更新履歴やアクセス不許可の履歴を記憶することによって、ＩＣカードに記憶された履歴を読み取ることができ、使用者自身でパスワードの更新管理やコンピュータシステムへのアクセス管理、所謂ログ管理をすることができる。

【００４５】

【発明の効果】以上説明したように本発明によれば、情報処理装置からの秘密情報及び符号化処理手順をＩＣカードで記憶し、ＩＣカードで特有となる秘密情報及びＩＤ情報並びにクロックにより計数した時間を、記憶された符号化処理手順に従って符号化し出力し、これを情報処理装置で復号し、復号された秘密情報と予め登録された秘密情報とが一致するとき、相互の接続を認めているので、秘密性が高い情報を安全性を確保しつつ授受することができる、という効果がある。

【図面の簡単な説明】

【図１】本発明の実施の形態にかかる、コンピュータシステムとＩＣカードとの各々の概略構成を示すブロック図である。

【図２】コンピュータシステム側で実行される処理の流れを示すフローチャートである。

【図３】ＩＣカード側で実行される処理の流れを示すフローチャートである。

【図４】期限切れ処理の流れを示すフローチャートである。

【図５】自動更新処理の流れを示すフローチャートである。

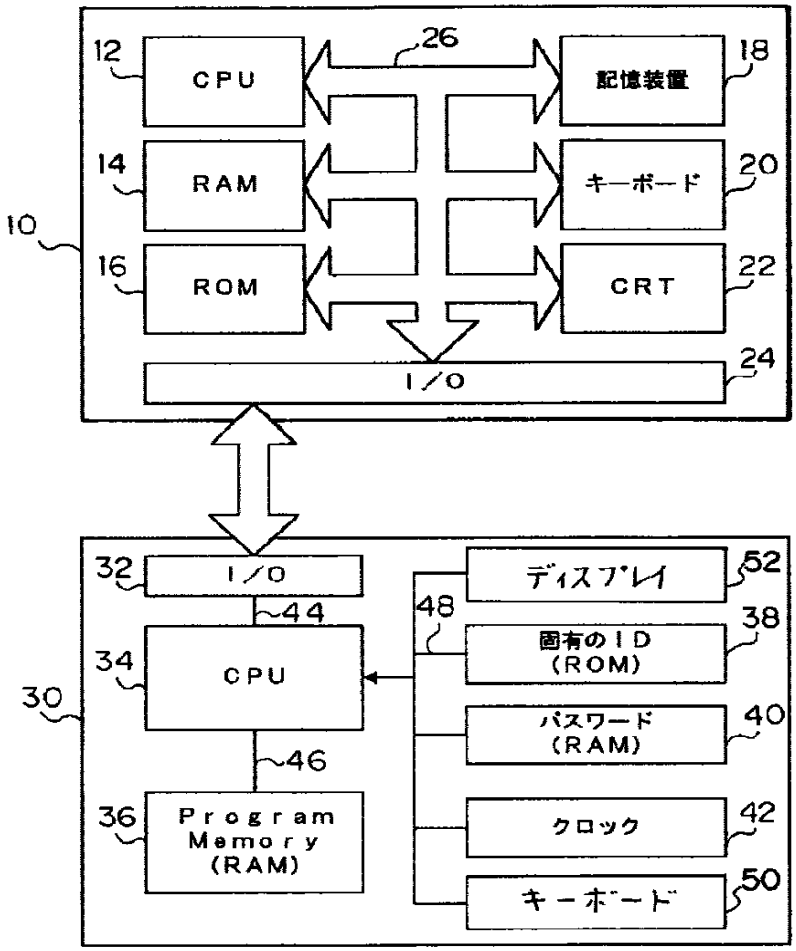
【図６】従来のセキュリティシステムを説明するための説明図である。

【図７】ＩＣカードの外観斜視図である。

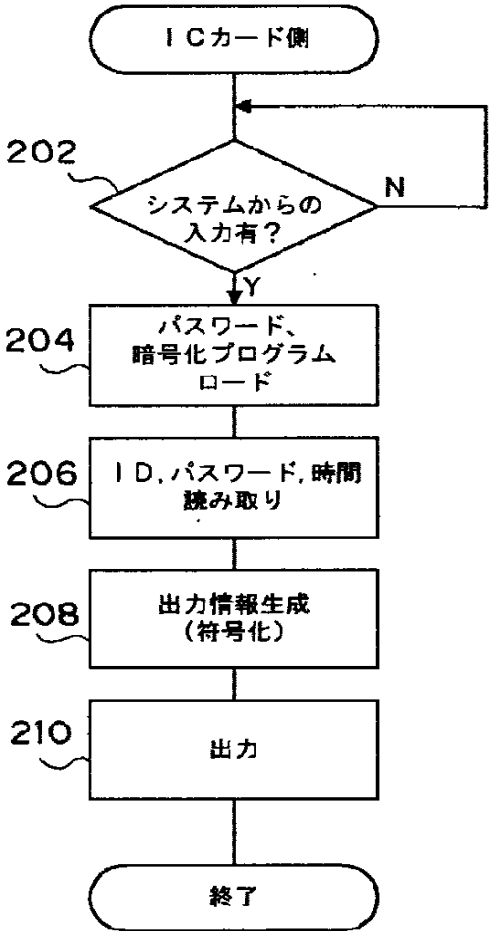
【符号の説明】

１０	コンピュータシステム
３０	ＩＣカード
３６	ＲＡＭ
３８	ＲＯＭ
４０	ＲＡＭ
４２	クロック

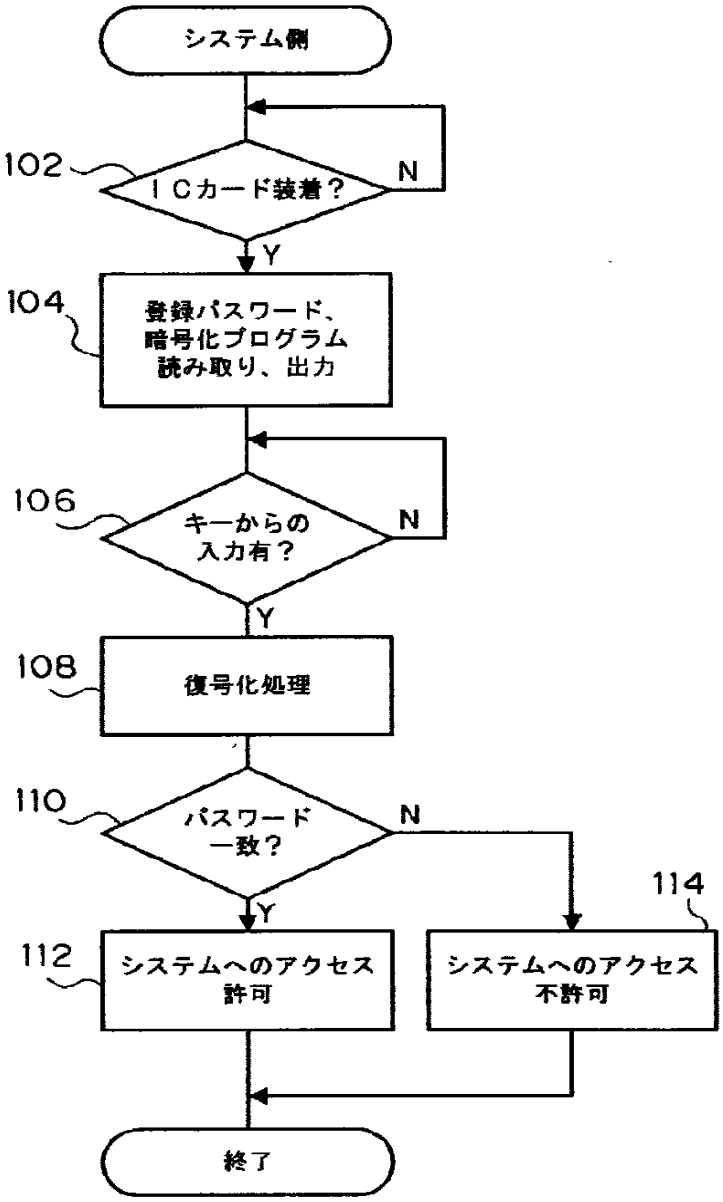
【図１】



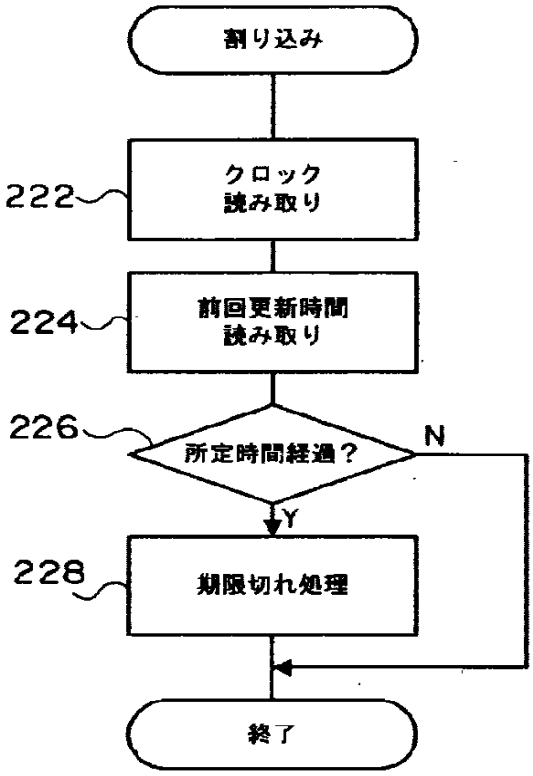
【図３】



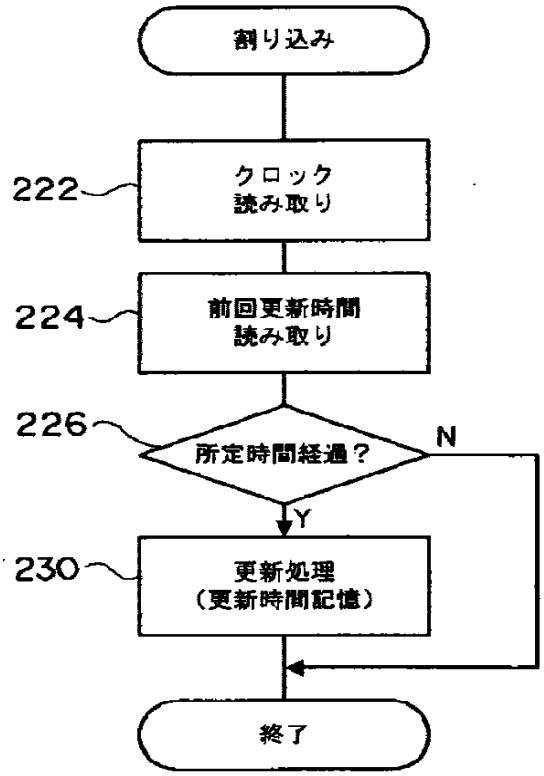
【図2】


システム側
102
ICカード装着？
N
Y
104
登録パスワード、
暗号化プログラム
読み取り、出力
106
キーからの
入力有？
N
Y
108
復号化処理
110
パスワード
一致？
N
Y
114
112
システムへのアクセス
許可
システムへのアクセス
不許可
終了

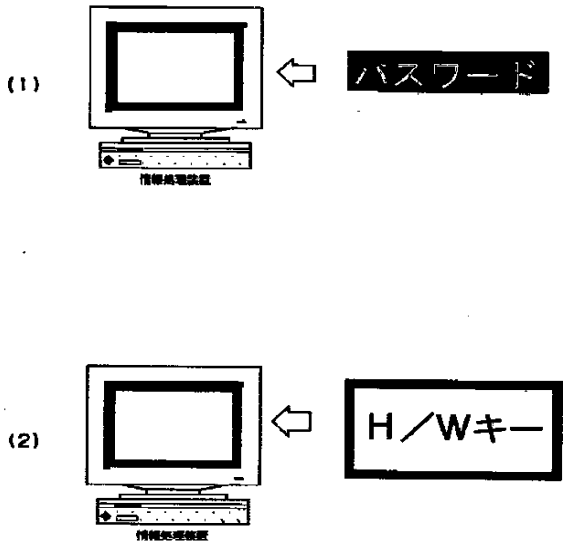
【図4】


割り込み
222
クロック
読み取り
224
前回更新時間
読み取り
226
所定時間経過？
N
Y
228
期限切れ処理
終了

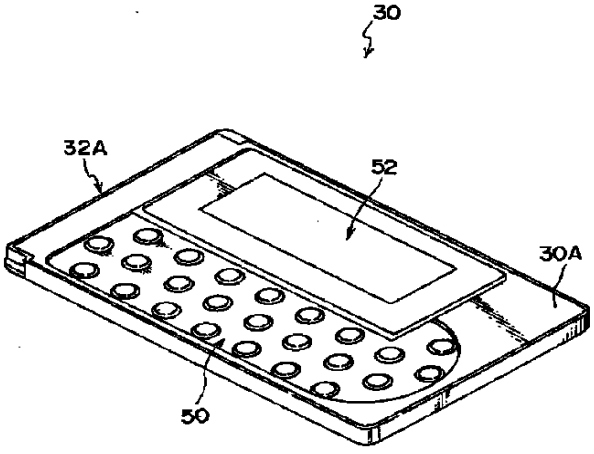
【図5】


割り込み
222
クロック
読み取り
224
前回更新時間
読み取り
226
所定時間経過？
N
Y
230
更新処理
（更新時間記憶）
終了

【図6】


(1)
パスワード
(2)
H／Wキー

【図7】


30
32A
52
30A
50

フロントページの続き

(51)Int.Cl.[6]	識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｈ０４Ｌ　9/32			Ｈ０４Ｌ　9/00	６７３Ｂ	
				６７３Ｅ	

(72)発明者　押山　隆
神奈川県大和市下鶴間1623番地14　日本アイ・ビー・エム株式会社　大和事業所内

IC CARD AND AUTHENTICATION METHOD OF INFORMATION PROCESSOR

Publication number: JP9114946

Publication date: 1997-05-02

Inventor: NISHINO KIYOSHI; OSHIYAMA TAKASHI

Applicant: IBM

Classification:

- international: ***G06F12/14; G06F21/00; G06F21/20; G06F21/24; G06K17/00; G06K19/07; G07F7/10; G09C1/00; H04L9/32;*** **G06F12/14; G06F21/00; G06F21/20; G06K17/00; G06K19/07; G07F7/10; G09C1/00; H04L9/32;** (IPC1-7): G06K17/00; G06F12/14; G06F15/00; G06K19/07; G09C1/00; H04L9/32

- European: G06F21/00N5A2D; G06F21/00N5A4; G07F7/10D4

Application number: JP19950255262 19951002

Priority number(s): JP19950255262 19951002

Also published as:

US5857024 (A1)

Abstract of **JP9114946**

PROBLEM TO BE SOLVED: To exchange high-secrecy information while securing safety by using an IC card. SOLUTION: An IC card 30 is provided with a ROM 38 holding an ID, clock 42, RAM 40 storing a password, RAM 36 storing an enciphering program and CPU 34 for executing processing, reads the stored ID and time (t) counted by the clock 42, enciphers these ID, password and time (t) according to the enciphering program, and outputs them to a computer system 10. At the computer system 10, the outputs from the IC card 30 are deciphered, the password is extracted, it is judged whether the deciphered password is coincident with a registered password or not and when they are coincident, access is permitted but when they are not coincident, access is not permitted.